韓國 컴퓨터情報學會 論文誌
第10卷 第1號, 2005. 3.

2005-3-1-1-17

보안 운영체제를 위한 강제적 접근 제어 보호 프로파일

고 영 웅*

Mandatory Access Control Protection Profile for Secure Operating System

Young-Woong Ko *

요 약

근래에 허가되지 않은 사용자로부터 공유된 자원에 대한 불법적인 접근이 빈번하게 이루어지고 있다. 접근 제어는 허가되지 않은 사용자가 컴퓨터 자원, 정보 자원 그리고 통신 자원을 이용하지 못하게 제어하는 것이며, 이처럼 허가받지 않은 사용자가 시스템 자원에 접근하는 것을 막는 것은 정보 보호에서 중요한 이슈로 떠오르고 있다. 본 논문에서는 접근 제어 정책 중의 하나인 강제적 접근 제어 메커니즘을 대상으로 TCSEC 보안 등급 B2 수준에 근접하는 보호 프로파일을 작성하였다. 본 연구 결과로 작성된 보호 프로파일은 정보 보호 시스템을 평가하는데 있어서 유용한 자료로 사용될 수 있다.

Abstract

Nowadays, it is possible to access sharing data from unauthorized people. Access control prevents unauthorized access to computing resource, information resources, and communication resources. It is very important to defend the critical system resources from the unauthorized. The importance of this study is to develop protection profile for Mandatory Access Control (MAC) that satisfies TCSEC assurance level B2. protection profile for MAC will help developers to use reference for the development of requirements and formulating security specification.

▸ Keyword : protection profile, access control, security

• 제1저자 : 고영웅
• 접수일 : 2005.01.31, 심사완료일 : 2005.03.07
* 한림대학교 정보통신공학부 조교수
This work was supported by the Research Grant(HRF-2004-42) from Hallym University, Korea

Ⅰ. 서 론

정보 통신 기술의 발달로 정보 시스템의 사용은 점차 늘어나고 있으며, 인터넷과 같은 정보 통신망에 대한 취약성 및 위험이 가중됨에 따라서 정보 보호에 대한 중요성이 크게 부각되고 있다. 정보 유출, 파괴, 위변조 등과 같은 컴퓨터 범죄 및 해킹이 급증하고 바이러스 감염, 서비스 방해, 불건전 정보 유통 등과 같은 정보화 역기능이 확산됨에 따라서 정보 보호 시스템에 대한 개념은 개인 및 기업 활동을 포함한 사회 전반에 있어서 중요한 이슈로 떠오르고 있다. 정보 보호 시스템은 정보를 적절하게 통제하여 불필요하거나 보증되지 않은 배포, 변경, 또는 손실과 같은 위협으로부터 정보를 안전하게 보호할 수 있어야 한다. 그러나 현재 널리 사용되고 있는 정보 보호 시스템들에는 신뢰할 수 없는 위험성이 내재하고 있으며, 이를 위해 정보 보호 시스템 내에 있는 위험성을 분석하고 위험성을 감수하거나 대처하기 위해 정보 보호 시스템을 평가할 수 있는 기준이 존재해야 한다. 현재 국제적으로 사용하고 있는 정보 보호 시스템 평가 기준[1-11]은 TCSEC(Trusted Computer System Evaluation Criteria) 및 ITSEC(Information Technology Security Evaluation Criteria) 등의 여러 평가 체계를 묶어 개발된 CC(Common Criteria)[2][3][4]라는 공통된 평가 기준이며 이를 사용하여 정보 보호 시스템을 평가하고 있다.

본 논문에서는 국제적인 공통 평가 기준인 CC에 기초하여 접근 통제 정책인 강제적 접근 제어(MAC: Mandatory Access Control)[12] 메커니즘을 대상으로 보호 프로파일(Protection Profile)[5]을 작성하는 과정과 방법에 대해서 기술하고, 결과물로 생성된 보호 프로파일의 유용성에 대해서 언급한다. 본 논문의 구성은 다음과 같다. 2장에서는 관련 연구로서 국제 공통 평가 기준 및 강제적 접근 제어에 대해서 언급하고, 3장에서는 보호 프로파일의 의미와 구성 내용에 대해서 구체적으로 설명한다. 4장에서는 강제적 접근 제어를 위한 보호 프로파일을 작성하는 과정을 기술하고, 마지막으로 5장에서 결론을 맺는다.

Ⅱ. 관련연구

2.1 국제 공통 평가 기준

CC는 기존의 다양한 평가 기준을 통합하여 1996년 1월 버전 1.0으로 개발되었고 1999년 8월에 현재의 최신 버전인 CC 2.1이 발표되었다. CC는 정보 보호 시스템의 보안 기능 요구 사항과 이를 평가하는 동안 적용하는 보증요구 사항에 대한 공통의 집합을 정하여 서로 독립적으로 수행한 평가 결과들을 호환할 수 있도록 하는 체계를 갖고 있다. CC는 크게 세부분으로 구성되어 있다. part 1은 소개 및 일반 모델을 제시하고 있으며 part 2는 보안 기능 요구 사항, part3는 보증요구 사항을 기술하고 있다.

2.1.1 보안 기능 요구 사항

보안 기능 요구(security functional requirement)에서는 가정된 TOE(Target of Evaluation)가 운영 환경에서의 위협에 대처하고 조직의 보안 정책을 적용하기 위한 보안 기능 요구 사항을 서술하고 있다. 보안 기능 요구 사항은 기능 클래스(class), 기능 패밀리(family), 기능 컴포넌트(component)의 집합으로 구성되어 있다. 클래스는 보안 요구 사항에 대한 가장 일반적인 그룹을 나타내며, 한 클래스내의 모든 구성 요소들은 같은 보안 목적을 가지는 반면 서로 다른 적용 범위를 가지고 있다. 클래스 내부에는 다양한 집합의 패밀리들이 존재하며, 패밀리는 보안 요구 사항들의 집합을 그룹화 한 것이다. 패밀리 내의 보안 요구 사항들의 집합은 같은 보안 목적을 공유하지만 요구 사항의 강조나 엄밀한 정도는 서로 다르다. 패밀리는 더욱 세부적으로 컴포넌트들의 집합으로 구성되며 컴포넌트는 보안 요구 사항의 특정 집합을 서술하며 국제 공통 평가 기준에서 정의한 구조를 포함하기 위해서 보안 요구 사항의 최소 집합을 선택할 수 있도록 하고 있다. 컴포넌트는 다수의 엘리먼트(element)들로 구성되어 있으며 엘리먼트는 보안 요구 사항을 가장 구체적인 수준으로 서술한 것이며 평가를 통해 각각의 보안 요구 사항을 검증할 수 있는 단위가 된다.

표 1. 보안 기능 요구 사항의 클래스 집합
Table. 1 Class of security functional requirement

클래스명	클래스 제목
FAU	보안감사(Security Audit)
FCO	통신(Communication)
FCS	암호지원(Cryptographic Support)
PDP	사용자 데이터 보호(User Data Protection)
FIA	식별 및 인증(Identification & Authentication)
FMT	보안 관리(Security management)
FPR	프라이버시(Privacy)
FPT	TOE 보안기능보호(Protection of TOE Security Functions)
FRU	자원활용(Resource Utilization)
FTA	TOE 접근(TOE Access)
FTP	안전한 경로/채널(Trusted Path/channel)

2.1.2 보증요구 사항

보증요구 사항(assurance requirement)은 TOE의 보증요구 사항을 표준화된 방법으로 표현한 것으로 보증 컴포넌트들의 집합을 정의하고 있으며 보증 컴포넌트, 보증 패밀리, 보증 클래스로 구성된다. 보증요구 사항에서는 보호 프로파일과 보안 목표 명세서에 대한 평가 기준을 정의하고 있으며 TOE평가를 EAL1에서 EAL7까지 7등급으로 나누고 있다.

2.2 강제적 접근 제어

본 논문의 목표는 접근 통제 정책인 MAC을 대상으로 하는 보호 프로파일을 작성하는 과정 및 결과의 유용성에 대해 고찰하는 것이며 이를 위해 접근 통제 정책 및 MAC의 개념에 대해서 간략히 기술한다. 접근 통제[12][13][14][15][16][17]라는 개념은 컴퓨팅 자원, 통신 자원 및 정보 자원 등에 대하여 허가되지 않은 접근을 방어하는 것을 목적으로 하며 여기서 허가되지 않은 접근이란 불법적인 자원의 사용, 노출, 파괴와 불법적인 명령어의 실행을 의미한다. 즉 접근 통제는 각 자원에 대한 기밀성, 무결성, 가용성 및 합법적인 이용과 같은 정보 보호 서비스에 직접적으로 기여하게 되며 이러한 서비스들의 권한 부여를 위한 수단이 된다. 대부분 컴퓨터 시스템의 사용자는 시스템을 사용하기 위하여 식별과 인증이라고 하는 검사 과정을 통해야 한다. 식별과 인증은 각 시스템 자원을 보호하기 위한 일차적인 보호 계층이 되며 접근 통제의 결정은 요청자의 신분이 완전히 인증되기 전까지는 수행될 수 없다. 인증이 성공하면 각 시스템 지원에 대한 사용자의 요청을 보안 정책이 적용된 접근 통제 절차에 따라서 허용여부를 인가받는다.

접근 통제 정책은 크게 규칙 기반 접근 제어 정책(mandatory access control, MAC)과 신분 기반 접근 제어 정책(discretionary access control, DAC)으로 나누어진다. DAC 정책은 특별한 사용자별로 정보에 대한 접근을 제공하고 추가적 접근 통제를 그 사용자에게 일임하는 방식이다. 이에 반하여 MAC 정책은 자동적으로 시행되는 어떤 규칙에 기반하고 있다. 그러한 규칙을 실제로 시행하기 위해 사용자와 대상에 대하여 광범위한 그룹 형성을 요구하고 있다.

III. 보호 프로파일 개요

보호 프로파일은 정보 보호 시스템을 이용하려는 소비자 혹은 정보 보호 시스템을 개발하려는 개발자가 정보 보호 시스템에 대한 보안 기능 요구 사항 및 보증요구 사항 등을 명세한 문서이다. 소비자나 개발자 혹은 정보 보호 시스템에 관심이 있는 제삼자는 보호 프로파일에 정보 보호 시스템에 대한 환경 및 정책, 목적, 기능 요구 사항과 보증요구 사항을 CC의 체계에 따라 기술할 수 있다. 보호 프로파일에서는 보안 목적을 충분히 만족시킬 수 있는 TOE에 대한 보안 요구 사항을 구현에 독립적으로 표현하는 것을 허용하고 있으며 이를 재사용할 수 있게 한다. 궁극적으로 보호 프로파일은 사용자에게 보안 필요성을 설명하는 수단을 제공하고 있으며 이러한 보안 필요성에 대한 평가를 손쉽게 할 수 있게 한다.

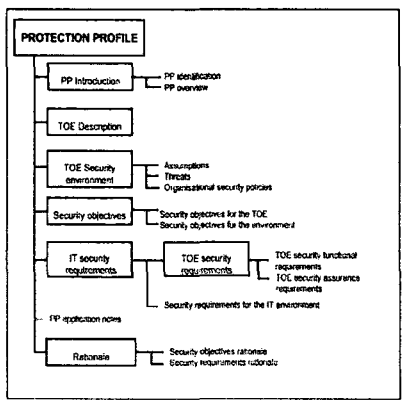

그림 1. 보호 프로파일의 구성
Fig. 1 protection profile layout

3.1 보호 프로파일의 내용

보호 프로파일은 그림 1과 같이 보호 프로파일 소개 (PP introduction), TOE 설명서(TOE description), TOE 보안 환경(TOE security environment), 보안 목적(security objective), 정보 보호 시스템의 보안 요구 사항(IT security requirement), 보호 프로파일 이용시 주의 사항(PP application notes), 이론적 근거(rationale)와 같은 내용으로 구성되어 있다.

보호 프로파일 소개에는 보호 프로파일을 등록하는데 필요한 보호 프로파일 식별 관련 정보와 보호 프로파일 개요에 대해서 기술되어 있다. 보호 프로파일 개요는 보호 프로파일의 잠재적 사용자가 보호 프로파일의 관심여부를 결정할 수 있도록 충분하고도 상세하게 설명되어야 하며, 보호 프로파일 목록과 등록에서 사용하기 위한 요약문으로 활용될 수 있다. TOE 설명서는 보안 요구 사항의 이해를 도모하기 위해서 TOE를 기술하고 있으며, TOE의 제품 유형이나 일반 정보 보호 시스템 특성에 대해서도 다루어야 한다. 보안 환경은 가정 사항, 위협, 조직의 보안 정책 등을 기술해야 하며, 가정 사항은 TOE를 사용하려는 의도가 있거나 사용이 예상되는 환경에 대한 보안 관점을 설명하며, 위협은 TOE와 TOE 환경에서 특별히 보호가 요구되는 자산에 대한 모든 위협을 포함시켜야 한다. 보안 정책 부분에서는 TOE가 따라야 하는 조직의 보안 정책 또는 규칙을 식별해야 하며, 보안 목적을 명백하게 하는 방법으로 각 정책별로 설명과 해석을 부여할 수 있다. 보안 목적에는 TOE와 TOE의 환경에 대한 보안 목적을 정의하여야 하며, 보안 목적은 보안 환경에서 식별되는 모든 관점을 다루어야 한다. 정보 보호 시스템 보안 요구 사항 부분에서는 TOE 보안 요구 사항과 시스템 환경에 대한 보안 요구 사항을 기술하게 된다. TOE 보안 요구 사항은 다시 TOE 보안 기능 요구 사항과 TOE 보증요구 사항으로 나누어진다. 보호 프로파일 응용시 주의 사항 부분은 선택사항이며, TOE에 관한 구성, 평가, 사용자에 대하여 유용하게 사용될 수 있거나 또는 관련된 추가 정보를 기술한다. 마지막 이론적 근거에서는 보호 프로파일의 요구 사항이 완전하고 종합적이라는 주장과 보안 환경 내에서 효과적인 정보 보호 시스템 보안 대책을 제공한다는 주장을 뒷받침 해줄 수 있는 증거물을 기술한다.

3.2 보호 프로파일 평가 현황

현재 보호 프로파일이 작성되어 CC에 의해 평가된 시스템은 대략 51개 정도이며 평가수준은 EAL1 등급에 해당되는 시스템 6개, EAL2 등급에 해당되는 시스템 20개, EAL3 등급에 해당되는 시스템 14개, EAL4 등급에 해당되는 시스템 11개가 존재한다. 이중 운영체제 제품 또는 접근 제어 관련 제품에 대한 평가는 8개가 존재한다.

표 2. 보호 프로파일 평가 제품 현황
Table. 2 Status of protection profile evaluation product

제품	보증 수준
Application Level Firewall Protection Profile for Basic Robustness Environments (v1.0)	EAL 2
Traffic Filter Firewall Protection Profile for Medium Robustness Environments (v1.4)	EAL 2
Role-Based Access Control Protection Profile Version 1.0	EAL 2
Application Level Firewall Protection Profile for Medium Robustness Environments (v1.1)	EAL 2
Traffic Filter Firewall Protection Profile for Low Risk Environments (v1.4)	EAL 2
Controlled Access Protection Profile	EAL3
Labelled Security Protection Profile	EAL3
Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile (v1.0)	EAL4

본 연구와 관련해서 대표적으로 알려진 "Smart Card Security Users Group Protection Profile v2.0"을 살펴보면 다음과 같다. 완전하게 재 작성된 Smart Card Protection Profile (SCPP) version 2.0은 Smart Card Security Users Group (SCSUG)에 의해서 작성되었다. 초기 vercion 1.0은 광범위한 공개적 검토에 의해서 최근에 발표되었으며, SCPP는 주요한 신용카드 금융 지불 시스템 (American Express, Europay, JCB, Master Card, Mondex, 그리고 Visa) 업체들과 NIAP에 의해서 작업되었다. SCPP는 스마트카드를 사용하는 금융 지불 시스템의 요구를 표현하고 있으며, 카드 발행 점과 최종 사용자에 초점을 맞추어 작성되었고, 하드웨어에서부터 다양한 응용 프로그램이 수행되는 운영체제에 이르기까지 전 범위에 걸친 안전한 스마트카드 플랫폼을 대상으로 하고 있다. SCPP에서 눈여겨 보아야 할 것은 스마트 신용 카드와 같은 단순한 금융 어플리케이션보다 잠재적으로 더 넓은 사용 범위를 가지고 있다는 것이다. 또한 TOE의 내부에서 위협과 보안 요구 사항들을 인지해냄으로써, 광범위하게 넓은 민감한 어플리케이션에 적용될 수 있도록 하고 있다. 예를 들어서 SCPP는 GSA의 "Smart Access Common ID Card" RFP를 위한 보안 요구 사항을 표현하는데 사용될 수 있다.

Ⅳ. 강제적 접근 제어를 위한 보호 프로파일 개발

보호 프로파일에 대한 명세 순서 및 구체적인 사항은 CC part1 annex B에 자세히 기술되어 있다. 보호 프로파일은 수작업으로 명세할 수 있지만 CCToolBox라는 도구를 이용하여 기본적인 내용을 작성하고 수 작업으로 퇴고를 하여도 된다. CCToolBox는 NIAP(National Information Assurance Partnership)에서 개발된 보호 프로파일 및 보안 목표 명세서의 명세 툴로서 보호 프로파일 및 보안 목표 명세서의 환경 변수 및 컴포넌트들을 효율적으로 관리해 주고 기본적인 내용을 문서화해주는 유용한 툴이다. 본 논문에서는 강제적 접근 제어 보호 프로파일을 작성하기 위하여, 보호 프로파일의 각 구성 요소 및 고려 사항을 체계적으로 기술하였다. 강제적 접근 제어를 위한 보호 프로파일인 MAPP(Mandatory Access Control Protection Profile)의 내용은 다음과 같다.

4.1 contents and presentation

이 부분에서는 보호 프로파일이 사용하는 CC의 버전 및 목차 그리고 MAC에 대해서 사용되는 용어를 기술한다.

4.2 introduction

보호 프로파일의 제목과 저자, MAC에 대한 간단한 설명 등을 기술한다.

4.3. TOE description

이 부분에서는 TOE가 갖게 되는 특성에 대해 서술한다. 본 보호 프로파일이 대상으로 삼는 TOE는 MAC이 구현되어 있는 일반적인 운영체제를 탑재한 정보처리 시스템이다. 또한 MAC이 안전하게 운용되기 위해 필요한 식별 및 인증, 감사(audit) 등이 구현되어 있는 운영체제를 대상으로 삼는다. 또한 정보처리 시스템은 일반적인 PC가 될 수도 있고 메인 프레임이나 웍스테이션 또는 분산 환경에서 돌아가는 여러 대의 서버를 대상으로 할 수도 있다.

4.4 TOE security environment

이 부분에서는 TOE가 운영될 환경에 대해 기술한다. CC에서 권고한대로 가정 및 위협, 보안 정책에 대해서 각각의 요소가 MAC이 구현된 환경에 어떻게 작용할 것인지에 대해 정의해야 한다. 이때 TCSEC division B의 mandatory protection 부분을 참조해서 각각의 요소들을 정의할 수도 있다. TCSEC division B에는 다른 어떤 문서들보다 MAC에 대한 정의 및 MAC이 운영될 환경에 대한 정책들을 자세히 정의해 놓았기 때문이다. 현재 만들어지고 있는 DAC 및 MAC에 대한 보호 프로파일의 대부분이 TCSEC의 MAC 및 DAC에 대한 정의에서부터 출발하고 있다[8].

모든 가정은 A라는 레이블로 시작하게 된다. 마찬가지로 위협과 보안 정책은 T와 P라는 레이블로 시작한다.

① 가정

CC에서 권고한대로 가정을 크게 나누어보면 physical assumption, personnel assumption, connectivity assumption 등이 있고 이 분류에 맞게 MAC에 적용될 각각의 가정을 생각해보면 다음과 같다. MAC에 관해서 physical assumption은 주로 외부의 공격에 대해서 물리적으로 대처할 수 있는 곳에 TOE가 존재해야 함을 가정해야 한다. personnel assumption은 유능한 관리자가 존재해야 함을 가정해야 하는데 MAC의 경우 관리자에 의해 그룹 및 객체의 보안 등급이 결정되므로 이 가정이 매우 중요한 요소가 된다. connectivity assumption에는 외부의 시스템도 같은 보안 정책 하에 있음을 명시해야 한다.

▶ Acc_to_Comms
시스템에 대한 통신의 물리적 방어는 허가받지 않은 접근이나 해킹 등을 막기 위해 적합하게 되어 있다.

▶ Phys_Acs_to_Out
TOE는 외부에서 허가받지 않은 물리적 접근을 차단하는 접근 장치 내에 위치해 있다.

▶ Competent_Admin
시스템 관리자는 TOE와 보안에 관련된 정보를 안전하게 관리할 수 있는 능력을 갖추어야 한다.

② 위협

위협의 구성요소에는 MAC에서 관리자의 역할이 중요하므로 관리자의 실수 및 권한 남용이 보안 정책에 중대한 영향을 끼칠 수 있다는 것과 MAC 시스템에 대한 외부의 해킹 위험이 존재함을 기술한다.

▶ Admin_Err_Omit
시스템 관리자는 보안에 관련된 중요한 기능을 수행하는

것을 실패할 수 있다.

③ 보안 정책

MAC을 기초로 한 정책을 우선 정하고 MAC이 운영되기 위해 부수적으로 필요한 정책들을 기술한다. 가령 P.classification에는 MAC의 기본적인 개념을 다루고 부수적으로 P.authorized_user에서는 권한을 받은 사용자만이 시스템에 접근할 수 있다는 것을 나타낸다. 또한 P.accountability에서는 인증 및 식별을 나타낼 수 있다.

▶ Authorized_Users
권한을 받은 사용자만이 시스템에 접근할 수 있다.

▶ Accountability
각각의 개인이 그들의 행동에 대해 책임을 져야 한다.

가정 및 위협 보안 정책에 관한 개념들은 한편 주관적인 것이므로 보호 프로파일 작성자가 왜 그런 개념을 정의했는지 rationale에 기술해주어야 한다.

4.5 security objectives

가정 및 위협, 보안 정책의 정의를 기초로 보안 목적을 정하게 된다. 보안 목적은 모든 위의 요소들을 모두 반영할 수 있어야한다. 예를 들어 P.authorized_user라는 정책을 정했으면 이에 맞는 O.authorized_user라는 보안 목적을 정의해 주어야 한다. 이렇게 가정 및 위협, 보안 정책과 보안 목적간에 매핑된 내용은 보호 프로파일의 rationale부분에서 기술해 주어야 한다. 보안 목적은 문맥에 따라 복수개의 가정 및 위협, 보안 목적과 매핑될 수도 있다. MAC에 관련된 보안 목적을 고찰해보면 authorization에 관련된 부분과 accountability, audit 그리고 MAC에 관한 분류로 나누어 기술할 수 있다.

▶ Authorization
TSF는 권한을 받은 사용자만이 TOE와 자원에 접근할 수 있음을 확신시켜야 한다.

▶ Enforcement
TSF는 보안 정책이 확실히 발효되도록 설계되고 구현되어야 한다.

▶ Info_Flow_Control
정보 흐름 정책을 사용자와의 의도와는 관계없이 강제적으로 집행해야 한다.

▶ User_Auth_Management
보안 정책에 따라 사용자 권한과 보안 데이터를 관리하고 업데이트 해야한다.

5.6 IT security requirement

보안 요구 사항 중 기능 요구 사항의 경우 보안 목적에서 정의한 사항들을 구현해 줄 수 있는 기능들로 구성되어야 한다. 보안 목적을 정의할 때 가정 및 위협, 보안 정책 등과 보안 목적을 매핑했던 것처럼 기능 요구사항을 선정할 때도 앞서 정의한 보안 목적의 주제에 맞추어 클래스 및 컴포넌트들을 선정해주어야 한다.

앞에서 고찰한 보안 목적의 범주에 authorization, accountability, audit, MAC 등이 있으며 여기에 적합한 클래스들을 선정해보면 FAU(security audit), FDP(user data protection), FIA(identification and authentication), FMT(security management), FPT(protection of the TSF), FTP(trusted path/channels) 등이 있다.

클래스들을 선정한 후에 컴포넌트들을 선정해주어야 한다. 컴포넌트들은 다음과 같은 기준으로 선정하면 도움이 된다. 본 논문이 목표로 하고 있는 MAC에 관한 보호 프로파일은 EAL5 등급이고 〈표 3〉과 같이 EAL5는 TCSEC B2 등급에 해당된다. CC와 TCSEC이 일대일로 기능 및 보증 요소가 매칭되는 것은 아니므로 〈표 3〉이 정확하다고는 볼 수 없다. 그러나 아래의 〈표 3〉이 일반적인 가이드라인이며 MAC의 경우 이미 TCSEC에 정의되어 있으므로 TCSEC의 B2 등급을 참조할 경우 컴포넌트들을 선정하는 시간을 절약할 수 있다.

표 3. CC 보안보증등급과 TCSEC과의 관계
Table. 3 Relation of CC security assurance level and TCSEC

EAL	설명	TCSEC
EAL1	functionally tested	
EAL2	structurally tested	C1
EAL3	methodically tested & checked	C2
EAL4	methodically designed, tested & reviewed	B1
EAL5	semiformally designed & tested	B2
EAL6	semiformally verified, designed & tested	B3
EAL7	formally verified, designed & tested	A1

▶ FDP_IFC.2 완전한 정보통제
FDP_IFC.2.1 TSF는 [할당: 주체와 정보 목록] 및 보안기능정책에 의하여 처리되는 통제된 주체나 주체로부터의 정보흐름에 대한 원인이 되는 오퍼레이션의 목록에 대하여

[할당: 정보흐름통제 보안기능정책]을 적용해야 한다.

FDP_IFC2.2 TSF는 통제범위 내에 있는 모든 주체나 주체로부터의 흐름에 대해서 TOE 통제범위 내의 정보 흐름의 원인이 되는 모든 오퍼레이션들이 하나의 정보흐름통제 보안기능정책으로 처리됨을 보장해야한다.

보안 요구사항에는 EAL5 패키지의 내용을 나열하면 된다.

- ATE_FUN.1.1D 개발자는 TSF를 시험하여 결과를 문서화하여야 한다.
- ATE_FUN.1.2D 개발자는 시험서를 제공하여야 한다.
- ATE_FUN.1.1C 시험서는 시험계획, 시험절차의 설명, 예상 시험결과 및 실제 시험결과로 구성되어야 한다.
- ATE_FUN.1.2C 시험계획에서는 시험하여야 할 보안기능을 식별하고 수행할 시험의 목적을 서술하여야 한다.
- ATE_FUN.1.3C 시험절차의 설명에서는 수행 예정에 있는 시험을 식별하고 각 보안기능을 시험하기 위한 계획을 서술하여야 한다. 이러한 계획은 다른 시험결과에 대한 순서 종속성을 포함하여야 한다.
- ATE_FUN.1.4C 예상 시험결과에서는 시험이 성공적으로 수행될 경우 예상된 결과를 보여야 한다.
- ATE_FUN.1.5C 개발자가 수행한 시험결과는 각각의 시험된 보안기능이 명시된 대로 동작함을 보여야 한다.
- ATE_FUN1.1E 평가자는 제공된 정보가 증거 요구사항을 모두 만족하는지 확인하여야 한다.

일반적으로 EAL 등급이 높을수록 정보 보호 시스템이 제대로 제작되고 테스트된다고 보장할 수 있지만 대신 시스템을 제작할 때 들어가는 비용은 더 높아지게 된다. 보호 프로파일을 작성할 때 정보 보호 시스템의 환경과 정보 보호 시스템의 가격을 고려하여 적당한 EAL 등급을 선택하려는 노력이 필요하다.

5.7 rationale

이 부분에는 보안 목적을 보안 환경에 매핑한 테이블과 보안 목적을 기능 요구 사항에 매핑시킨 테이블을 첨부하고 그 이유에 대해서 설명을 해야 한다.

V. 결론

본 논문에서는 정보 시스템에서 널리 사용되고 있는 강제적 접근 제어에 대한 보안 요구 사항을 국제공통평가기준에 따라서 기술하였으며, 이러한 결과로 보호 프로파일을 작성하였다. 본 연구 결과에 기술되어 있는 보호 프로파일은 TCSEC 기준 등급 B2급에 해당되며, 보호 프로파일을 이용하여 정보 시스템 구매자, 개발자, 평가자들이 기대하는 보안 수준을 만족시키는지 평가하는 자료로 사용될 수 있다. 뿐만 아니라, 본 연구에서 기술하고 있는 보호 프로파일의 작성 과정은 다양한 정보 보호 시스템의 보안 요구 사항을 기술하는 보호 프로파일을 작성하는데 참고로 사용될 수 있다.

참고문헌

[1] Arrangement on the Mutual Recognition of Common Criteria Certificates in the field of Information Technology Security, 1998.10

[2] CCIB, Common Criteria for Information Technology Security Evaluation - Part 1 : Introduction and general model, 1998.5

[3] CCIB, Common Criteria for Information Technology Security Evaluation - Part 2 : Annexes, 1998.5

[4] CCIB, Common Criteria for Information Technology Security Evaluation - Part 3 : Security assurance requirements, 1998.5

[5] ISO/IEC JTC 1.27.22, Guide for Production of PPs and STs, Version 0.6, 1998.7

[6] NIST, NSA, Evaluation and Validation Scheme for Information Technology Security, 1998.10

[7] NIST, Information Security Testing - Common

Criteria, 1998.9
[8] ASD, Department of Defense Trusted Computer System Evaluation Criteria, 1985. 12
[9] CEMEB, Common Evaluation Methodology for Information Technology Security - Part1 : Introduction and general model, 1997.1
[11] CEMEB, Common Evaluation Methodology for Information Technology Security - Part2 : Evaluation Methodology, 1997.9
[12] William M.Daley, Cary R.Bachula, Raymond G.Kammer, NIST Handbook-xx : Information Technology Security Common Criteria V1.0, 1998.9
[13] Ingrid M. Olson, Marshall D. Abrams, "Computer Access Control Policy Choices", Computer & Security, Vol. 9, pp.699-714, 1990.
[14] Harrison M.A., Ruzzo W.L., Ullman J.D., "Protection in operating systems", Comm. ACM, 19(8), pp.461-471, 1976.
[15] Simon Garfinkel, Gene Spafford, "Practical UNIX Security", O'Reilly and Associates, 1994.
[16] Harrison M. A., Ruzzo W. L., Ullman J.D., "Protection in operating systems", Comm. ACM. 1976.
[17] 손우용, 송정길, "통합보안관리 시스템에서의 침입탐지 및 대응을 위한 보안 정책 모델에 관한 연구", 컴퓨터정보학회논문지, 2004. 6.
[10] 고병수, 박영신, 최용락, "컴퓨터포렌식스를 지원하는 보안 감사/추적 모듈 설계", 컴퓨터정보학회논문지, 2004. 3.

저 자 소 개

고영웅

1997년 고려대학교 컴퓨터학과 졸업(학사)
1999년 고려대학교 대학원 컴퓨터학과(이학석사)
2003년 고려대학교 대학원 컴퓨터학과 (이학박사)
2003년~현재 한림대학교 정보통신공학부 컴퓨터공학과 조교수
〈관심분야〉 멀티미디어/실시간 운영체제, 보안 운영체제